



Managing Skype for Business:

QoS with LiveNX



Product Disclaimer: LiveAction has renamed their software solution, formerly known as "LiveAction" to "LiveNX." From 2016 and on, LiveNX will remain the official name for the software solution.

TABLE OF CONTENTS

Microsoft Skype for Business Overview	
Microsoft Skype and the Role of QoS	4
Microsoft Skype QoS Design	5
Define TCP/UDP Port Ranges	5
Client-to-Client Settings	5
Microsoft Skype Phone Edition Settings	6
Microsoft Skype Server Settings	6
Microsoft Skype Edge Server Settings	7
Define Group Polices	7
Microsoft Skype DSCP Marking Group Policies	
Network QoS Configuration	11
How Does QoS Work?	11
What is LiveNX?	
Microsoft Skype Audio QoS Classification with LiveNX	
Microsoft Skype Audio QoS Queuing with LiveNX	25
Microsoft Skype Video QoS with LiveNX	
Appendices:	
Appendix A: LiveNX ACL Management for Skype	
Appendix B: Skype With Cisco Performance Monitoring	
Appendix C: Skype QoS Audio Configuration Using NBAR2 Definitions	
Appendix D: Skype QoS Queuing with LiveNX and NBAR2	
More Information	
About LiveAction	

MICROSOFT SKYPE FOR BUSINESS OVERVIEW

Microsoft[®] Skype[®] for Business (formally known as Lync[®]), part of Microsoft Office 365, is an enterprise-level collaboration solution for instant messaging, presence, conferencing, file sharing, and telephony. While Skype for Business is a simple application to use, protecting Skype voice and video call quality throughout the network can be difficult. Fortunately, a network administrator can effectively implement Quality of Service (QoS) protection for Skype using LiveAction's application-aware network performance management solution, LiveNX.

LiveNX utilizes Cisco's advanced features to simplify implementation of these management controls through a rich Graphical User Interface (GUI). LiveNX provides a comprehensive management solution for monitoring, troubleshooting and provisioning Skype QoS to ensure that bandwidth is properly allocated to support your enterprise's needs. Users can take advantage of LiveNX to virtually go back in time to perform analysis and troubleshooting for real-time or historic Skype calls utilizing the Medianet Performance Monitor Path Analysis feature.

This document describes how you can easily protect critical Skype audio and video traffic throughout the network with LiveNX. You'll learn how to:

- Configure Skype audio and media ports and markings at the Clients and Server
- Use LiveNX to verify Skype traffic through the network
- Use LiveNX to create Access Control Lists (ACLs) for Skype
- Use LiveNX to configure QoS Marking Policy
- Use LiveNX to configure QoS Queuing Policy
- Use LiveNX to monitor performance of Skype

By using NBAR2 (protocol pack 12 or higher), Cisco's application recognition technology built into IOS, Skype QoS management can be further simplified to uniquely identify Skype audio and video without having to configure Microsoft Skype Servers for QoS, Microsoft Group Policies for QoS, or build and manage complex ACLs in the network infrastructure.* This can translate to 50% faster (or higher) QoS deployments and reduces the chance of mistakes during the configuration. LiveAction highly recommends updating to this protocol pack to simplify a Skype QoS deployment (see Appendix D for further details).

MICROSOFT SKYPE AND THE ROLE OF QOS

Microsoft Skype is an application that allows enterprise users to communicate via instant messaging (IM), presence, audio/ video conferencing, IP telephony, and collaboration tools. Communication occurs between Skype clients that have installed the Skype software on their PC, MAC or mobile devices (Windows, iPhone/iPad, Android). Other communication devices may also communicate via Skype (PSTN, IP phones, IP video conference unit). The enablement of these communication technologies is dependent on several Skype servers. Each server has a specific role in the Skype operation. The roles can be co-located on one server or installed on multiple servers to add high availability and scaling capabilities. These roles are:

- Front-End Servers
- Back-End Servers
- Mediation Servers
- Edge Servers

By default, Skype clients and servers do not set QoS markings on their data. Additionally, Skype client-to-client communication does not use a defined range of TCP/UDP ports. Since the network infrastructure cannot recognize Skype traffic by port or QoS marking in its default state, it cannot prioritize these flows as they traverse the network.* This can cause performance impact to both Skype voice and video traffic on highly utilized enterprise networks.

To ensure Skype always receives the QoS priority it needs, it must first be configured to set QoS markings on its traffic as it is sent onto the network. Microsoft has published white papers on their website for enabling QoS on Skype traffic. <u>Visit here</u> for more details.

These documents can be summarized into two primary steps:

- 1. Set uniform TCP/UDP port ranges that Skype applications will utilize
- 2. Set QoS markings on Skype clients and servers based on the port ranges above

This means that network administrators must configure the appropriate QoS markings by application (VOIP, VIDEO, etc.) for each client and server that participates in a Skype solution. There are three types of Skype communications: client-to-client, client-to-server, and server-to-server. Each application must be configured for these communications scenarios. Fortunately, centrally configured shell commands and Microsoft Group Policy can manage these configurations.

Once the Skype clients and servers have been configured to set the appropriate QoS markings for Skype data, the network infrastructure that these applications traverse must also be configured to support the level of call quality required to meet business objectives. This is done by the configuration of IP QoS to all applicable network devices (routers and switches) that transmit and receive Skype voice and video.

The management and configuration of QoS in networks can be very complex to operate, manage and validate. It can require reviewing hundreds of lines of Command Line Interface (CLI) commands to understand the configuration and performance of QoS polices on just one device alone. Therefore, understanding end-to-end QoS policies on an enterprise network can become extremely difficult at best. LiveNX has been designed to streamline the implementation and management of QoS in network environments and can be used to easily deploy this complex set of technologies to the network infrastructure.

*Cisco has updated its NBAR2 application recognition technology to granularity recognize Skype audio and video. By using NBAR2 protocol pack 15 (or higher) on the application Cisco routers and LiveNX, it is possible to easily protect Skype audio and video via just the network infrastructure. This means it is possible to eliminate the need for any changes on Microsoft servers or clients as outlined in this document (see Appendix D for further details).

This document will provide the configuration parameters required to configure Skype for Business 2016 clients and servers. It will also detail the required steps of implementing QoS in a network infrastructure. Finally, this document will highlight how a network infrastructure's QoS can be configured, monitored and validated using LiveAction software.

Microsoft Skype QoS Design

The following diagram shows a typical Skype enterprise deployment.



Define TCP/UDP Port Ranges

The first step in deploying QoS for Skype is to define the TCP and UDP port numbers that the Skype applications will use. These port numbers should be configured in a consistent way so all devices that participate in Skype will use the same ports for each application type–for example, VOIP could always use ports 20000-2099, video 21000-21099, etc.

Client-to-Client Settings

To configure client-to-client port use, you can use the following shell commands on the Skype Front-End Server. Once these parameters have been set, Skype clients should log off and back on to the Skype client to acquire these new settings. The following commands are a valid example of how to configure these settings:

Set-CsConferencingConfiguration -ClientMediaPortRangeEnabled \$True Set-CsConferencingConfiguration -ClientAudioPort 20000 -ClientAudioPortRange 100 Set-CsConferencingConfiguration -ClientVideoPort 20100 -ClientVideoPortRange 100 Set-CsConferencingConfiguration -ClientAppSharingPort 20200 -ClientAppSharingPortRange 100 Set-CsConferencingConfiguration -ClientFileTransferPort 20300 -ClientFileTransferPortRange 100

These can be entered via: Start > All Programs > Microsoft Skype Server 2016 > Skype Server Management Shell

WHITE PAPER

Microsoft Skype Phone Edition Settings

The default QoS DSCP value of Skype Phone Edition is 40. In most environments the DSCP value for audio traffic is 46. To update this configuration, issue the following command:

Set-CsUCPhoneConfiguration -VoiceDiffServTag 46

This can be entered via: Start > All Programs > Microsoft Skype Server 2016 > Skype Server Management Shell

Microsoft Skype Server Settings

To configure client-to-server and server-to-server port use, you could use the following shell commands on the Skype Front-End Server. These settings update the Skype Conference, Application, and Mediation servers. Once these parameters have been set, the appropriate Skype services will need to be restarted to apply these new settings. The following commands are a valid example of how to configure these settings:

```
Set-CsConferenceServer -Identity <ConferenceServer:FQDN of Skype Pool> -AudioPortStart 21000
-AudioPortCount 1000
Set-CsConferenceServer -Identity <ConferenceServer:FQDN of Skype Pool> -VideoPortStart 22000
-VideoPortCount 1000
Set-CsConferenceServer -Identity <ConferenceServer:FQDN of Skype Pool> -AppSharingPortStart 23000
-AppSharingPortCount 1000
Set-CsApplicationServer -Identity <ApplicationServer:FQDN of Skype Application Srv. Pool>
-AudioPortStart 21000 -AudioPortCount 1000
Set-CsMediationServer -Identity <MediationServer:FQDN of Skype Mediation Srv. Pool>
-AudioPortStart 21000 -AudioPortStart 21000
```

These can be entered via: Start > All Programs > Microsoft Skype Server 2016 > Skype Server Management Shell

MICROSOFT SKYPE EDGE SERVER SETTINGS

The Skype Edge servers do not need to have any ports reconfigured, as they will rely on the other Skype devices inside the network for port selection. Note that DSCP markings only need to be set for private Skype traffic. Any DSCP values marked on Skype traffic that traverse the Internet will typically have these priority settings ignored by all service providers.

Define Group Polices

Once the Skype port settings have been assigned to all applicable device types via the Skype Server Management Shell, DSCP markings can be set by implementing Group Polices for these applications' port ranges. To implement a QoS Group Policy, navigate to a computer that has Group Policy Management installed, locate the container where the new policy should reside (e.g. client OU), right-click on the container and select "Create GPO in this domain, and link it here." The following screenshots will display how to configure the appropriate Group Policy for Skype Audio. This is applicable for Windows 7, 8, and Vista clients.

First, name the policy and specify the DSCP value.

Policy-based QoS	X
Create a QoS policy A QoS policy applies a Differentiated Services Code Point (DSCP) value, throttle rate, or both to outbound TCP, UDP, or HTTP response traffic. Policy name:	
Skype Client Audio	
Specify DSCP Value:	_
Specify Outbound Throttle Rate:	
Learn more about QoS Policies < gack Next > Cancel	æ



Define the application to which this policy applies.

Policy-based QoS
This QoS policy applies to: <u>All applications</u> <u>Qnly applications with this executable name:</u>
Skype.exe
Example: application.exe or %ProgramFiles%\application.exe
Only HTTP server applications responding to requests for this URL:
Include subdirectories and files
Example: http://myhost/training/ or https://*/training/ Example of non-standard TCP port: http://myhost:8080/training/ or https://myhost:*/training/
Learn more about QoS Policies
< Back Next > Cancel

Specify the source and destination address to which this policy applies.

licy-based QoS	l
Specify the source and destina	ion IP addresses.
A QoS policy can be applied to IPv6) address or prefix. For HT client(s) that issued the HTTP r	utbound traffic that is from a source or to a destination IP (IPv4 or IP response traffic, the destination IP address or prefix denotes the equest.
This QoS policy applies to:	
Any source IP address	
O Quely for the following source in the following s	IP address or prefix:
This QoS policy applies to:	
Any destination IP address	
Only for the following destin	ation IP address or prefix:
Example for a host address Example for an address pre	1.2.3.4 or 3ffe:ffff::1 fix: 192.168.1.0/24 or fe80::1234/48
Learn more about QoS Policies	
	< Back Next > Cancel



Select the protocol and port ranges that this policy matches with and click "Finish."

Policy-based QoS	
Specify the protocol and port numbers. A QoS policy can be applied to outbound traffic us range, or a destination port number or range. Select the protocol this OoS policy applies to:	ing a specific protocol, a source port number or
Specify the source port number:	
From this source port number or range:	20000:20099 Example for a port: 443 Example for a port range: 137:139
Specify the destination port number:	
<u>To any destination port</u>	
⑦ To this destination port number or range:	
Learn more about QoS Policies	
	< Back Finish Cancel

Microsoft Skype DSCP Marking Group Policies

The same process will need to be repeated for all other Skype clients and servers (Conferencing, Mediation, Application). Please use the table below as a sample reference for defining Skype TCP/UDP ports and Group Polices. The port numbers used in this example would be valid for an environment with up to 500 simultaneous conference users.

Group Policy Name	Application Executable	DSCP	TCP/UDP	Src IP	Dst IP	Src Ports	Dst Ports
Skype Conferencing Server Audio	AVMCUSvc.exe	46	Both	Any	Any	21000-21999	
Skype Conferencing Server Video	AVMCUSvc.exe	34	Both	Any	Any	22000-22999	
Skype Edge-Server Internal Audio–Clients	MediaRelaySvc.exe	46	Both	Edge Internal IP	Any		20000-20099
Skype Edge-Server Internal Audio–Servers	MediaRelaySvc.exe	46	Both	Edge Internal IP	Any		21000-21999
Skype Edge-Server Internal Video–Clients	MediaRelaySvc.exe	34	Both	Edge Internal IP	Any		20100-20199
Skype Edge-Server Internal Video–Servers	MediaRelaySvc.exe	34	Both	Edge Internal IP	Any		22000-22999
Skype Mediation Server Audio	MediationServerSvc.exe	46	Both	Any	Any	21000-21999	
Skype Application Server	OcsAppServerHost.exe	46	Both	Any	Any	21000-21999	
Skype Client Audio	Skype.exe	46	Both	Any	Any	20000-20099	
Skype Client Audio 2010	Communicator.exe	46	Both	Any	Any	20000-20099	
Skype Client Video	Skype.exe	34	Both	Any	Any	20100-20199	
Skype Client Video 2010	Communicator.exe	34	Both	Any	Any	20100-20199	

Note: These ranges may not be appropriate for all network designs.

NETWORK QOS CONFIGURATION

Microsoft Skype relies on the network infrastructure to honor and queue its traffic for call quality protection. The following pages will describe the steps required to implement and validate these QoS polices in a network infrastructure using LiveNX.

How Does QoS Work?

QoS is a suite of technologies used to manage bandwidth usage as data crosses computer networks. Its most common use is for the protection of real-time voice or video communications and high-priority data applications. QoS technologies, or tools, each have specific roles that are used in conjunction with one another to build end-to-end network QoS policies.

The two most common QoS tools used to handle traffic are classification and queuing. Classification identifies and marks traffic to ensure network devices know how to identify and prioritize data as it traverses a network. Queues are buffers in devices that hold data to be processed. Queues provide bandwidth reservation and prioritization of traffic as it enters or leaves a network device. If the queues are not emptied (due to higher priority traffic going first), they overflow and drop traffic.

Policing and shaping are also commonly used QoS technologies that limit the bandwidth utilized by administratively defined traffic types. Policing enforces bandwidth to a specified limit. If applications try to use more bandwidth than they are allocated, their traffic will be remarked or dropped. Shaping defines a software set limit on the transmission bandwidth rate of a data class. If more traffic needs to be sent than the shaped limit allows, the excess will be buffered. This buffer can then utilize queuing to prioritize data as it leaves the buffer.

The Weighted Random Early Discard (WRED) technology provides a congestion avoidance mechanism that will drop lower priority TCP data to attempt to protect higher priority data from the adverse effects of congestion.

Finally, link-specific fragmentation and compression tools are used on lower bandwidth WANs to ensure real-time applications do not suffer from high jitter and delay.



Table 1: Packet flow through a typical QoS policy

WHAT IS LIVENX?

LiveNX is an application-aware network performance management tool that will graphically display how networks and applications are performing using SNMP and the latest advanced NetFlow capabilities now embedded in Cisco devices. In addition to showing application and network performance, LiveNX provides the ability to control application performance via its graphical QoS management capabilities. In the following, LiveNX will be used to highlight how easily QoS can be configured to manage and control Skype audio and video traffic. Moreover, this document will describe how LiveNX can be used to confirm the application performance of Skype using the latest Performance Monitoring technology now available in some Cisco devices.

The image below is a view of the LiveNX console. It shows a network diagram consisting of two Skype clients and three network devices. The three larger green circles represent routers and switches managed by LiveNX. The little green circles within the devices represent their interfaces.



Microsoft Skype Audio QoS Classification with LiveNX

Since LiveNX is also a NetFlow collector, it has the ability to graphically visualize the traffic that is flowing over the network. In the diagram below, the light blue arrows represent Skype audio traffic traversing the network. In this example, the color legend below shows that the light blue arrows represent Best Effort traffic. This is what one would expect to see before any



QoS configuration is implemented on the Skype servers and clients as described previously in this document.

Double-clicking on any of the larger circles (routers/switches) in the LiveNX network diagram will show the real-time NetFlow data of traffic that is flowing through the device. In the example below, the Skype traffic's UDP port numbers are not in the administrator's defined port ranges and the DSCP values are Best Effort. This confirms that the Skype servers and clients have not yet be been configured appropriately for QoS.

Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	In IF	Out IF	DSCP and	Dst
JDP	192.168.6.3	21,841	222.222.222.222	22,168	ms-lync-media	Vlan 1	FastEthernet	0 (BE)	4
JDP	192.168.6.3	21,841	222.222.222.222	22,168	ms-lync-media	Vlan1	FastEthernet4	0 (BE)	-
JDP	123.123.123.	2 161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	4
JDP	123, 123, 123,	2 161	192, 168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
JDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
JDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
JDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
JDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
JDP	192.168.6.2	51,849	2.2.2.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
-					1.0		<u>e iei</u> ia		

WHITE PAPER 🔊

After the appropriate Skype QoS settings have been implemented on the Skype servers and clients, the network diagram will show red arrows, in addition to the light blue arrows. This indicates EF or high priority markings are now being set on Skype audio traffic. But notice in the example below, the red arrows are not being drawn through the whole Skype conversation path. This indicates that the network infrastructure's QoS trust policy is not configured correctly.



This can be confirmed if one was to double-click on the device that is showing the red arrows painted through it. In the LiveNX real-time NetFlow view below, the UDP ports are in the appropriate range and the DSCP value is EF.

	Chable Folling	i elle rause c	Dasic Tiow	• •	Deraditi inter di di	φ • •		Colors + En	uroina
Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	In IF	Out IF	DSCP and	. Dst
UDP	192.168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vian1	FastEthernet	46 (EF)	-
UDP	192.168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vlan 1	FastEthernet-	46 (EF)	-
UDP	123.123.123.	2 161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	9 (BE)	-
UDP	123, 123, 123,	2 161	192, 168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan 1	FastEthernet4	0 (BE)	-
UDP	192, 168, 6, 2	51,849	123.123.123.2	161	snmp	Vlan 1	FastEthernet4	0 (BE)	-
UDP	192.168.6.2	51,849	2.2.2.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
1		F1 040			11			a (nr1	

If instead one double-clicked on one of the devices showing just blue arrows, the UDP ports would be in the appropriate ranges, but the DSCP value would still be 0.

Q Q	🛞 Enable Polling	Pause (Display Basic Flow	- 🖙	*DefaultFilterGroup	- 6	Display Filter	Colors - Er	nd Point
Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	In IF	Out IF	BSCP and .	Dst
UDP	192.168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vlan1	FastEthernet	0 (BE)	-
UDP	192.168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vlan1	FastEthernet-	0 (BE)	-
UDP	123.123.123.	2 161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	8 (BE)	-
UDP	123, 123, 123,	2 161	192, 168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.2	51,849	123, 123, 123, 2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.2	51,849	2.2.2.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
	100 100 0 0	F1 040						a (pr1	

The previous screenshots validate what the LiveNX network diagram was indicating; the DSCP value of 46(EF) is being lost by some type of misconfigured QoS trust policy in the network. To investigate this network QoS issue further, the administrator should start the troubleshooting process on the last device that shows the intended QoS markings. In this example, this would be the first device on the left with the red arrows passing through it (shown below). Fortunately the LiveNX application doesn't stop at just showing the Skype QoS problems, but gives administrators the ability to fix the QoS issue with its graphical QoS management tools.





To access these tools, click the "QoS" tab at the top left of the LiveNX network diagram and then double-click on the device that needs QoS configuration investigation (the device to the left in this example).



This will show a list of interfaces managed on this device. Notice in the screenshot below that on the Ethernet 0/0 interface, there is a QoS policy named "SET_DSCP" configured in the input direction.

A		LiveAction - 198.18.1	33.34		_ 0 ×
File View Users GoS Flow	Bouting IP SLA LAN Tools Reports Help				
Dashboard Manage Depand	QoS Flow Routing IP SLA LAN				
Q.	G Enable Poling				
Name	Name	Policy	Bandwidth(kbps)	Class drop	
🕀 🕭 Home	Ethernet0/0	SET DSCP		1.047	
OatsCenter_Core	0.004			751	•
G Ethernet0/2	e 9 Ethernet0/2			752	
OataCenter-WAN_EDGE	-I Output	QUELEING		1,086	•
Ethernet0/0					
E 🛞 Remote_Site					
Ethernet0/0					
CPU CPU Memory CPU Plow Buffer CPU	Alerts Advisories Modes C			a	admin: Admin user 12:16:59 AM POT

To further investigate this policy, right-click on the policy's name > select QoS > Manage QoS Settings.

ashboard Manage 🗊 Expand	QoS Flow Routing IP SLA LAN BEnable Polling	
ame	Name	Policy
	Crownerstown Characteristics - Crownerstown Characteristics	ISET_DSCP eate Policy from Template djust Input QoS djust Output QoS anage QoS Settings

This will bring up a new window (shown below) that will allow the administrator to configure all required QoS policy settings via LiveNX's GUI.

Select the policy named "SET_DSCP" in the list to the left. This will show a list of the classes applied to this policy. In this example, there is only one class named class-default. Click on "class-default" to highlight it. Notice how this policy is currently marking all traffic (via the class-default) with a DSCP value of 0, Best Effort.

A Manag	e QoS Sett	ings - Da	ataCenter_	Core.dclo	oud.cisco	o.com (1	98.19.1.1)			×
J I A A A A A										
Policies Classes Interfaces										
Policies	Mapped Class	ses								
LIVEACTION-POLICY-MEDIANET LIVEACTION-POLICY-UNIFIED	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
B→C QUEUEING B→C SET DSCP Cassidefault	Mapped Class Drop all to Classify M	s Detail raffic for da	ISS	ing Shanin	a Compr	ession WD	FD DBI Lins	unported		
			cocing Point	ang anapin	g compr	casion we				
	Match on: A	ny		Edi	t		Ref Cli cri me cri the all the	ass is defi iteria show atch-any: eet at least iteria to be e class. atch-all: p criteria to e class.	ned by v at left packet t one of a mem packet r be a m	the must the ber of nust meet ember of
< >										
Help					Save to	Device	Preview C	11	(Close



This policy needs to be fixed to allow Skype traffic's DSCP markings to pass through this device unchanged— that is, the DSCP value of 46 will be seen across all infrastructure devices to ensure consistent QoS handling of Skype traffic across the network. To do this, first right-click on the "SET_DSCP" policy and select "Add Class to Policy." This will bring up a new window, as shown below. Create a new class called "SKYPE_AUDIO."

Δ .	Add Class to Policy
Select one of the follow	ing options:
O Use existing dass:	4C_BL_CriticalData_App-Match_Mark v
Create new class:	SKYPE_AUDIO
Note: This option w select the "Class ta	ill create an empty class. You will need to b* to add classification parameters.

The new class will be added to the SET_DSCP policy. Match criteria needs to be defined to ensure the appropriate traffic uses this class. Click the "Edit" button on the "Classify Tab."

A Manag	je QoS Setting	s - DataCenter	_Core.dcld	oud.cisco	o.com (1	98.19.1.1)			×
ତ୍ର କା 💽 🖏 🖓 🗞 🦠									
Policies Classes Interfaces									
Policies	Mapped Classes								
UVEACTION-POLICY-MEDIANET	Class Name C	assify Marking	Oueueina	Policing	Shaping	Compression	WRED	DBL	Unknown
LIVEACTION-POLICY-UNIFIED	SKYPE_AU	•							
SKTPE_AUDIO dass-default	class-default	•							
	Mapped Class De	tail							
	Drop all traffi	c for class							
	Classify Markin	ng Queueing Pol	icing Shapin	ng Compr	ession WF	RED DBL Unsi	upported		
	Match on: Any					Ref	erence		
						Cla	teria shov	at left	the
						M	atch-any:	packet	must
						me	et at least teria to be	one of a mem	the ber of
						the	class.		
			Ed			Ma all the	atch-all: p criteria to e class.	acket n be a m	nust meet ember of
< >									
Help				Save to	Device	Preview C	u	(Close

This will bring up the "Create and Edit Match Statements" configuration page. Select "DSCP" from the "Match Type" dropdown.



Select a "Value" of "46(EF)" and click "Add Match Statement."

A Manage	QoS Settings - DataCenter_Core.dcloud.cisco	o.com (198.19.1.1)
4 4 2 2 2 2 2		
Policies Classes Interfaces		
Classes Create and Edit Ma	tch Statements	
🗣 🖻 🕱 🛛	0.000	Match any w
4C BL CriticalDat	DSCP	
4C_BL_Realtime_A Value:	42	 M Match T Value
4C_BL_Scavenger	43	
4C-MN_CONTROL	44	
4C-MN_CRITICAL	45 (EE)	
4C-MN_REALTIME	47	
LIVEACTION-CLAS	48 (CS6)	
RDP	49	~
SKYPE_AUDIO	(Select up to 8 values)	
Match/match not:	Match	~
	TPv4 Only	
	Add Match Statement	t
< >		
Help	Save to	Device Preview CLI Cancel

LiveAction

The DSCP value will now appear in the far right column, indicating it is a valid match type for this class. Click "Save to Device."

A Manage	QoS Settings - DataCenter_Core.dcloud.cisco	o.con	n (198.19.1.1)	×
41 41 🞝 🖏 🖏 🗞 %					
Policies Classes Interfaces					
Classes Create and Edit Mai	tch Statements				
🔁 🖻 🕱 🛛	lasen.	_	Match any w	199	
Match type:	DSCP	~	Plater any v	~	
4C_BL_Realtime_A Value:	42	^	M Match T.	Value	
4C_BL_Scavenger	43		Ma DSCP	46 (EF)	
4C-MN_CONTROL	44				
4C-MN_CRITICAL	45				
4C-MN_REALTIME	40 (EF)				
LIVEACTION-CLAS	48 (CS6)				
PDP	49	~			
SKYPE_AUDIO	(Select up to 8 values)				
Match/match not:	Match	~			
	IPv4 Only				
	Add Match Statement Replace Match Statemen	nt			
< >					
Hala	Carro M	Devie	Drawie		Canad
nep	Save u	o Devic	- C- Preva	ew CLI	Cancel

Click on the "Policies" tab to the top left of the screen to review the changes made to the SET_DSCP policy. Notice DSCP value 46(EF) is now a match type of the SKYPE_AUDIO class. This would fix this QoS issue. But what if this network has other VOIP traffic marked EF too?

It would also match this class intended for Skype audio traffic. Since this is a classification and marking policy at the network edge, it would be best to ensure that only Skype audio matches this class. To enforce this, a second match type needs to be added to this class and the class needs to use the "Match All" setting (to use AND logic). To make these changes, click the "Edit" button.







Select Match Type "ACL Name."

A Manag	e QoS Settings - DataCenter_Core.dcloud.cisco.co	om (198.19.1.1)
4422265		
Policies Classes Interfaces		
Classes Create and Edit M	atch Statements	
🕒 🗈 🕱 Match type	: ACL Name	Match any 🗸 🞇
4C_BL_Croitcaluat 4C_BL_Realtime_/ Value 4C_BL_Scavenger	Any ACL Name ACL Number	M Match T Value Ma DSCP 46 (EF)
4C-MN_CONTROL 4C-MN_CRITICAL 4C-MN_REALTIME	Class COS DSCP	
LIVEACTION-CLAS LIVEACTION-CLAS RDP	Frame relay DE bit Frame relay DLCI BTD Protocol - using NBAP	
SKIPE_AU010 Match/match no	: HTTP Protocol - using NBAR -input interface ID Procedence MAC Destination Address MAC Source Address MPLS experimental topmost Packet length Protocol - using NBAR Protocol - using NBAR Protocol - using NBAR Protocol - using NBAR Protocol - using NBAR	
< >>	Save to Dev	

Select an access list that matches the UDP ports used for Skype client and server audio. In the example shown below, there is already an access list available called "SKYPE_AUDIO_ACL." Select this access list and click "Add Match Statement." See Appendix A for more information on how to create and manage access lists using LiveNX.

A Manage	QoS Settings - DataCer	nter_Core.dcloud.cisco.co	om (198.19.1.1)	×
4488865				
Policies Classes Interfaces				
Classes Create and Edit Mat	ch Statements			
AC BL CriticalDat	ACL Name	~	Match any 🗸 💥	
HC_BL_Realbuck Value: HC_BL_Realbuck_/ Value: HC_BL_Scavenger HC_MN_CONTROL HC_MN_CONTROL HC_MN_REALTIME	Value: BEST_EFFORT CRITICAL DEVI_GLOBAL_LEARN_LIST LIVEACTION-ACL-AVC RDP		M Match T Value Ma DSCP 46 (EF)	
LIVEACTION-CLAS	SKYPE_AUDIO_ACL SKYPE_VIDEO_ACL VOICE_VIDEO			
SKYPE_AUDIO Match/match not:	Match	~		
	Add Match Statement	Replace Match Statement		
< >				
Help		Save to Dev	vice Preview CLI	Close



Select "Match All" from the drop-down at the top center of the screen. Click "Save To Device."



Click on the "Policies" tab to validate both match criteria and the "Match on All" is configured appropriately. If everything is valid, click "Close."



Click "Home" in the device list to the left to return to the network diagram view. Click the "Flow" tab and click the "Refresh" button. As long as the previous example is the only network QoS issue, all arrows will now show as red for this Skype conversation. This means that all devices see Skype traffic marked with a DSCP value of 46(EF), high priority.



These QoS settings can be confirmed by double-clicking on any of the devices that show red arrows painted through them. In the LiveNX real-time NetFlow view below, the UDP ports are in the appropriate range and the DSCP value is EF.

al al	Enable Polling	Pause D	Display Basic Flow	- 4	*DefaultFilterGroup	- 6	Display Filter	Colors -	End Poin
Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	In IF	Out IF	DSCP and	Dst
JDP	192.168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vlan1	FastEthernet	46 (EF)	-
JDP	192, 168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vlan1	FastEthernet	46 (EF)	
JDP	123.123.123.	2 161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	8 (BE)	-
JDP	123.123.123.2	2 161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	2
JDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
JDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
JDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
JDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
JDP	192.168.6.2	51,849	2.2.2.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
		F		404		1.0			

Note that this QoS classifying and marking example provided is very simple. The steps shown need to be repeated throughout the network environment to ensure all Skype client and server audio DSCP markings are honored appropriately.

Microsoft Skype Audio QoS Queuing with LiveNX

Once Skype audio traffic has been classified and honored as high priority (DSCP 46(EF)) end-to-end in the network, steps should be taken to ensure Skype traffic is prioritized appropriately. The diagram below shows Skype traffic being marked appropriately (as red) end-to-end.



This prioritization needs to happen at any congestion point in the network. Congestion occurs most often at the WAN edge, but can also happen in the LAN. When implementing a QoS queuing policies, start where the problem occurs most, the WAN edge. The following pages will show how to configure a queuing policy using LiveNX to prioritize Skype traffic at the WAN edge.

First, click the "QoS" tab and then double-click the middle device (in this example the data center WAN edge device).



This brings up a list of the interfaces on this device. In this example, there are no QoS polices applied to any interface. To create a queuing policy, right-click on an interface and go to QoS > Manage QoS Settings.

A		LiveAction - 1	98.18.133.34		_ 0 ×
<u>File View Users Gos Flow</u>	Bouting IP SLA LAN Tools Reports Help				
Dashboard Manage DEpand	QoS Flow Routing IP SLA LAN				
Q	G Enable Poling				
Name	Name	Policy	Bandwidth(Kbps)	Class drop	
Tane 3 € terret0 ↓ € terret0	None ● € Characti() ● ● ● Statution ● <td>Paky</td> <td>EandoudPróbago</td> <td>Class drap 249 308 372 292</td> <td>6 6 6</td>	Paky	EandoudPróbago	Class drap 249 308 372 292	6 6 6
K S OU © Henry © For Suffer ©	Tode ©				dem: Advenuer 12-41:37 AVR01

This brings up the Manage QoS Settings window, as seen below. To create a new policy, click the "Add Policy Button" at the top left of the page.

Policies	Mapped Classes	
C LIVEACTION-POLICY-UNIFIED	Class Name Classify Marking Queueing Polking Shaping Comprete Mapped Class Detail	Ission WRED DBL Unknow Unsupported Reference
		Class is defined by the criteria show at left. Match-any: packet must meet at least one of the criteria to be a member of the class. Match-all: packet must mee all criteria to be a member of



In this example, the new policy will be named QUEUEING.

A	Add Policy	×
Policy nar	me: QUEUEING	
	OK	Cancel

Right-click on the policy and add a new class to the policy. This new class will be called VOIP.



A	ŀ	dd Class to Polic	y	×
Select one o	f the follow	ng options:		
O Use exis	ting class:	4C_BL_CriticalData_A	App-Mato	ch_Mark ∨
Create r	new class:	VOIP		
Note: Th select th	iis option w e "Class tal	create an empty class " to add classification (s. You w paramete	ill need to ers.
		C	ж	Cancel

LiveAction

Add match criteria as described above to match EF to the VOIP class.

A Manage C	QoS Settings - Data	Center-W	AN_EDGE.	dcloud.	cisco.con	n (198.19.2.1)		
Polices Pol	Mapped Classes	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
	Mapped Class Detail Drop all traffic for c Classify Marking Q	lass ueueing Pol	licing Shapir	ng Compr	ession WF	RED DBL Uns	upported		
	Match on: Any					Ret	erence		
\rightarrow	Match : DSCP : 46 (E	F)				Cl cr M me cr th	ass is defi teria show atch-any: eet at leas teria to be e class. atch-all: p	packet packet a mem packet r	the must the ber of nust meet
< >			Ed	it		all the	criteria to e class.	be a m	ember of
Help				Save to	Device	Preview C	u [(Close

Click the queuing tab and select the queuing type "Priority." Set the bandwidth percentage to 33%. This is a safe starting number for this queue and can be adjusted by monitoring the queues performance over time. See below for examples of how to monitor this queue.

A Manage C	oS Settings - Data	Center-W	AN_EDGE.	dcloud.o	isco.con	n (198.19.2.1)		×
🔁 🖲 🜲 🖨 🕷 🗞									
Policies Classes Interfaces									
Policies	Mapped Classes								
🛃 🕷 😹 🗛 🐘 🛝 🕸	P3 🗈 📑 🖮								
ELIVEACTION-POLICY-MEDIANET	Class Name Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
UVEACTION-POLICY-UNIFIED	VOIP 🔶		Priority: 3						
VOIP	dass-default 👳								
- dass-default									
	Mapped Class Detail								
	Drop all traffic for c	lass							
	Classify Marking Q	eueing Po	licing Shapir	na Compr	ession WF	RED DBL Uns	upported		
						Daf	erence		
	Queueing type: Prior	ity 🗸				Dis	stribute the	e availa	ble ^
	Rate: 33	Percer	nt 🗸			ba	ndwidth b	etweer	1
	Burst size:	12	bytes			Cla	isses by a nimum bar	dwidth	ng a
	Unknown element	s:				gu	arantee to	each o	class.
						Q	eueing '	Туре	
						CI	ass-base	d: utiliz	es
						Cla	ass-based	weigh	ted fair
						de	rived wei	ght for p	packets
						fro	m the bar	dwidth	~
< >						<	and the	Pore	>
Help				Save to	Device	Preview C	u	(Close

Click on the "Interface" tab, right-click on the output of interface Ethernet 0/2 (the WAN interface) and apply the QUEUING policy.

Ethernet0/0 Cutput : <none> Output : <none> Outpu</none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none>	Interface name: Ethernet0/2 IP address: 10.255.2.2 IP address mask: 255.255.0 Interface description: cy to Interface Maximum reserved bandwidth: 75 0 %	Apply Policy to Interface
Vulput: <none> Vulput: <none> Vulput: <none> Output: <none> Output:</none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none>	* This device supports HQF, therefore reserved bandwidth settings are Pre-classify Link Fragmentation: Maximum delay: ms Interleave	mace_global QUEUEING POLICE INFACTION-POLICY-MEDIANET

Click "Save to Device" and "Close." Skype audio traffic will now be given priority treatment when this WAN interface becomes congested.



To verify Skype's performance return to the network diagram, click the "Home" icon at the top left of the screen, then select the "QoS" tab, and double-click on the Ethernet 0/2 interface. The graph and legend to the bottom of the screen shows the real-time performance statistics of this new QoS policy. This screenshot confirms that 46(EF) traffic (Skype in this example) is being protected by the VOIP queue.



To see this same information historically click the "1hr" button to the top of the screen to run a historical report for this policy's performance. Click the "Custom" button to view this policy for an administratively defined time range. In the historical report shown below, notice how the "Post-Policy Report" shows traffic in the VOIP queue (Skype in this example) at 210kbps. This matches with the real-time report above.





Another QoS historical report that is useful for monitoring QoS performance is the "Pre-Policy and Post-Policy Drops" Report. The "Class drops" graph and legend will show, which queues have been dropping any traffic. In this example there are no drops in the VOIP queue, this validates that Skype traffic is performing optimally on this interface for the time range shown.

	QoS Reports	- 0
2- Type here to Blar reports Reports Device CPU/Memory Usage Interface Bandwidth Interface Bandwidth Compa	Pre-Policy and Post-Policy Drops The 6h 1d July 300d 900 Jy Custom	
-Interface/Interface Drops -NBAR Comparison	DataCenter-WAN_EDGE v - Ethernet0/2 v Outbound	v Execute Report
Pre-Policy and Post-Policy Pre-Policy and Post-Policy C Pre-Policy and Post-Policy C Pre-Policy and Post-Policy E Top CPU Usage Top Memory Usage	Show Total Bandwidth Pre-policy	Before QoS - by Class in Klops Options *
Top Interface Bandwidths Top Interface Drops	4,000	QUEDENS V
- Top Class Bandwidte - Top Class Dropps - Top Class Dropps - Top Class Dropps - Top Class Dropps - Top Class - Top Class - Ste Walt Top Top - Ste Alert - Ste Alert Detail Custom Raports	3,000 \$2 \$2,000	Name Average Pas
	1,000- 0 Jul 26, 1006 50 AM Jul 26, 1006 50 AM Jul 26 Class drons	. 10.06: 10 Ам с т , т , т , т , т , т , т , т , т , т
	ciuss urops	QUELEING
t Actions As Internet of the CSV	<u>ک</u> ۲.000	Name Average Peak

Microsoft Skype Video QoS with LiveNX

The steps to configure and confirm Skype video application performance are very similar to the steps shown for Skype audio. The task required will be summarized below.

First, ensure Skype video is classified and matched appropriately. This would include ensuring Skype video traffic is trusted as it enters the network edge. Using the example from the Skype audio section of this document, add a "SKYPE_VIDEO" class to the SET_DSCP policy. It is recommended to use "Match on ALL" for both the DSCP value and ACL to ensure only Skype traffic matches this class.

A Manag	ge QoS Settings - DataCenter_Core.dcloud.cisco.com (198.19.1.1)								
ସ 🗐 🔊 🖏 🖣 🗞 🦻									
Policies Classes Interfaces									
Policies	Mapped Classes								
LIVEACTION-POLICY-MEDIANET LIVEACTION-POLICY-UNIFIED	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unknown								
	SKYPE_VIDEO								
dass-default	dass-default 👳 DSCP: BE								
	Mapped Class Detail Drop all traffic for class								
	Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported								
	Match on: Any Reference								
	Match : DSCP : 34 (AF41) Class is defined by the criteria show at left. Match : ACL Name : SKYPE_VIDEO_ACL Match-any: packet must meet at least one of the criteria to be a member of the class.								
	Match-all: packet must meet al criteria to be a member of the class.								
د >									
Help	Save to Device Preview CLI Cancel								





Once the appropriate trust configuration is in place, LiveNX will validate that the DSCP value is marked end-to-end by showing the colored arrows across the network map. In the example below, the red arrows indicate Skype audio (EF) and the gold arrows indicate Skype video (AF41).

Once DSCP markings are confirmed to be honored through the network end-to-end, Skype video should be prioritized on the appropriate network devices. Using LiveNX's QoS tools, create a new video class on the same queuing policy that was created for Skype audio. Configure the class to match on DSCP 34(AF41).

A Manage C	QoS Settings - DataCenter-WAN_EDGE.dcloud.cisco.com (198.19.2.1)
 Policies Classes Interfaces 	
Policies	Mapped Classes
UVEACTION-POLICY-MEDIANET UVEACTION-POLICY-UNIFIED UVELEING VOIP VIDEO VOIP VIDEO dass-default	Class Name Class Name Class Name Class Name Compres WRED DBL Un VOID Priority: 33% VIDEO Class-based: 20% Class-base
	Mapped Class Detail Drop all traffic for class Classfer Lange Classific Longer Lange Classific
	Match on: Any Reference
	Metch : DSCP : 26 (AF31) Class is defined by the criteria show at left. Match-any: packet must meet at least no of the class. meet at least no of the class. Edit Edit
< >	
Help	Save to Device Preview CLI Cancel

Configure this VIDEO class to queue traffic. In this example, the video class will be assigned 20% as a CBWFQ.

A Manage C	QoS Settings - DataCent	ter-WAN_EDGE.dcloud	d.cisco.con	n (198.1	19.2.1)			×
J I I I I I I I 6 5								
Policies Classes Interfaces								
Policies	Mapped Classes							
🛃 🖷 🖹 🔝 🌆 🖷 🖏 🕫	🖳 🔂 📑 🖮							
IVEACTION-POLICY-MEDIANET	Class Name Classify Ma	arking Queueing	Policing S	Shap (Compres	WRED	DBL	Un
LIVEACTION-POLICY-UNIFIED	VOIP 👻	Priority: 33%						
VOIP	VIDEO	Class-based: 20%						
	Cass-default 👳							
dass-default								
	Mapped Class Detail							
	Drop all traffic for class							
	Classify Marking Queueir	Policing Shaping Con	npression W	RED DBL	Unsuppor	ted		
	Queueing type: Class-bas	ed			Reference	e		
	Quedening type: Class bas				Distribut	te the ava	ailable	^
	Rate: 20	Percent v			bandwid	dth betw	een	
	Queue depth: 1	Bytes 🗸			classes	by spec bandwi	ifying a dth	
	Enable Fair Queue	ing			guarant	ee to eac	h class	.
	Unknown elements:		_		0	an Tan		
					Queue	ing Type	•	- 11
					Class-b	based: u	tilizes inhted f	air
					queuein	g (CBWF	Q) usin	9
					derived from the	weight f	or pack	ets
					allocated	d to the c	lace	~
< >					<			>
Help		Save	to Device	Pre	eview CLI		Cance	1

Once the video queue is created, its operation can be confirmed by viewing the interface's QoS statistic. In the example, below, video traffic is being matched in the bottom graph in purple.





APPENDICES:

Appendix A: LiveNX ACL Management for Skype Appendix B: Skype with Cisco Performance Monitoring Appendix C: Skype QoS Audio Configuration Using NBAR2 Definitions Appendix D: Skype QoS Queuing with LiveNX and NBAR2



APPENDIX A: LIVENX ACL MANAGEMENT FOR SKYPE

LiveNX has ACL management capabilities that allow administrators to configure and push access lists to the enterprise. This gives engineers the ability to centrally manage and deploy ACL in their network. To manage the access list on a device, right-click on the device, select "Device Tools," and "Manage ACLs."

Δ			LiveAction - 198.18.1	33.34		_ 5 ×
Eile View Users Gos	Flow B	outing IPSLA LAN Tools Reports Help				
Dashboard Manage 🕃 E	pand	QoS Flow Routing IP SLA LAN				
Q.		(@ Chable Poling)				
Name		Name	Policy	Bandwidth(Opps)	Cass drop	
D CataCenter Cont	_	- Input	SET_DSCP		1,094	
@ Ethernet0/0	evice: Data	Center_Core.dcloud.clsco.com				
Ethernet0/2 DataCenter-W	Beer		OFFENS		759	
G Ethernet0,0	Paulies					
G Ethernet0/2	IR GLA					
Ethernet0/0	IAN					
G Ethernet0/1	Edd Day	ine Settings				
	Add or 8	lemove Interfaces				
	Refresh	Device				
	Remove	Device				
	Zoom te	n Device				
	Device Tools		Save to Startup Config			
	Statistics +		Open Device Web Page			
	View .		Manage ACLs			
	Group N	fanagement +	57			
CPU © Memory © Flow	>	lette 🔍 Advisones 🔍 Nodes 🔍				admin: Admin user 01:16:26 AM PO

A list of the ACLs found on the device will appear. Click on one of the access lists to see its configuration at the bottom of the screen. Click the "Edit ACL" button to manage the access list. The example ACL below shows the information that would match Skype Audio in this document.

Current Router	DataCenter_C	lore		
Access Contro	Lists (ACLs)			
Name / Number	^	Туре	Applied Interfaces	Create ACL
ACL-BITTORREN	T-PC1	Extended (Named)		Educe N/
ACL-CITRIX-PC1		Extended (Named)		
CL-FTP-PC1		Extended (Named)		Delete ACI
CL-G711-19420)	Extended (Named)		boccence
CL-INET-PUBLI	С	Extended (Named)		Copy ACL
EST_EFFORT		Extended (Named)		
RITICAL		Extended (Named)		Apply / Remove ACL
ENY_GLOBAL_L	EARN_LIST	Extended (Named)		-
IVEACTION-AC	L-AVC	Extended (Named)		
DP		Extended (Named)		
KYPE_AUDIO_A	ACL	Extended (Named)		
KYPE_VIDEO_A	CL	Extended (Named)		
VOICE_VIDEO		Extended (Named)		
Access Rule En	itries			Save ACL File
				Load ACL File



Select one of the ACL rules and click "Edit Rule" to update the variables as appropriate.

	Edit Extended ACL SKYPE_AUDIO_ACL	×
Туре	Extended \lor	
Name / Number	SKYPE_AUDIO_ACL	Help
Remarks		Create Remark
		Edit Remark
		Remove Remark
Access Rules		
permit ip any any		Create Rule
		Edit Rule
		Copy Rule
		Delete Rule
		Maria
		Move Up
		Move Down
	Preview CLI Save to	Device Cancel

Edit the ACL as requited and click "OK" when finished.

Edit Extended Rule Entry for SKYPE_AUDIO_ACL	×
 ● permit of deny ● TCP ● UDP Object-Group < No Object Groups > ▼ Other by Name Source ● any of by Network or IP ● by Object-Group ● c.g 192.168.1.0/24 or 192.168.1.19 ✓ No Object Groups > ▼ ✓ by Port Between ▼ Manage Port(s) << 	v ahp v Destination o any by Network or IP e.g 192.168.1.0/24 or 192.168.1.19
Match by DSCP v v	OK Cancel



The ACL referenced above can be used as the match criteria for a QoS policy (as shown below).

A Manag	ge QoS Settings - Data	Center_Core.dclc	ud.cisco.com	(198.19.1.1)		×
 Policies Classes Interfaces 						
Policies	Mapped Classes					
	P3 🖿 🚯 🖮					
LIVEACTION-POLICY-MEDIANET	Class Name Classify M	larking Queueing	Policing Shapi	ng Compression	WRED DBL	Unknown
	SKYPE_AU					
SKYPE AUDIO	class-default DS	SCP: BE				
SKYPE_VIDEO						
class-default						
	Mapped Class Detail					
	Drop all traffic for class					
	Classify Marking Queue	ing Policing Shapin	g Compression	WRED DBL Uns	upported	
	Match on: All			Re	ference	the
	Match : DSCP : 46 (EF) Match : ACL Name : SKYPE	E_AUDIO_ACL		cr	iteria show at lef	t.
				M	atch-any: packe	t must
				m	eet at least one o	fthe
				cr th	iteria to be a men e class.	nber of
					atch-all: nacket	must meet
				al	criteria to be a n	nember of
		Edi	t	th	e class.	
< >						
Help			Save to Device	Preview 0	au 🗌	Close

Below is another example ACL. This example shows the information that would match Skype video in this document.

	ACL Manageme	nt for DataCenter_Core	×
Current Router DataCente	er_Core		
Access Control Lists (ACL	s)		
Name / Number	Туре	Applied Interfaces	Create ACL
ACL-BITTORRENT-PC1	Extended (Named)		Edit ACI
ACL-CITRIX-PC1	Extended (Named)		Edit ACL
ACL-FTP-PC1	Extended (Named)		Delete ACL
ACL-G711-19420	Extended (Named)		
ACL-INET-PUBLIC	Extended (Named)		Copy ACL
BEST_EFFORT	Extended (Named)		
CRITICAL	Extended (Named)		Apply / Remove ACL
DENY_GLOBAL_LEARN_LIST	Extended (Named)		
LIVEACTION-ACL-AVC	Extended (Named)		
RDP	Extended (Named)		
SKYPE_AUDIO_ACL	Extended (Named)		
SKYPE_VIDEO_ACL	Extended (Named)		
VOICE_VIDEO	Extended (Named)		
Access Rule Entries			
permit udp any range 20100 20) 199 any		Save ACL File
permit dup any range 22000 2	2999 dily		Load ACL File
			Close



APPENDIX B: SKYPE WITH CISCO PERFORMANCE MONITORING

LiveNX supports the Cisco Performance Monitoring Flexible NetFlow template. This will allow administrators to deploy and manage Performance Monitoring in the network infrastructure and gather application performance metrics (packet loss, jitter) for voice and video over IP. This advancement in technology gives administrators the ability to understand how these applications are performing without the use of probes or other costly network appliances. Using the technology now embedded inside Cisco network equipment, voice and video call quality issues can be detected and reported to network administrators before end-users ever complain.

The first step in gaining this visibility into voice and video application performance is to enable this flow type in the Cisco network infrastructure. LiveNX can automate these tasks and enable the deployment of this complex set of configurations in a simple point-and-click manner. This can be done with the following step:



From the Menu bar, Select Flow > Configure Flow.

LiveAction

Check the devices to enable the Voice/Video Performance (Medianet) flow type and click "Configure Selected." In this example, all three devices are checked.

A			Flow Co	onfiguration					-	• ×
Instruct	ions t devices to configure flow									
Flow Co	nfiguration Table									
Q.										
Select	Device	Туре	IP Address	Description	Tags	Traffic	Applic	Voice/Vid	Traditi	Custom
	DataCenter-WAN_EDGE	Standard 🗸	198.19.2.1	Cisco IOS S	WAN,	•	۲	۲	۲	0
	DataCenter_Core	Standard v	198.19.1.1	Cisco IOS S	WAN,	•	•	۲	•	•
	Remote_Site	Standard v	198.18.129.25	Cisco IOS S	WAN,	•	•	۲	•	•
	Help						Configure	Selected	Ck	ose

Check the box of the desired technology on each interface and click "Save to Devices." In this example, all interfaces have FNF (basic Flexible NetFlow) and Voice/Video Performance (Medianet) selected.

			FI	ow C	onfigurat	ion		_	
Instructions Configure the type of flow you	wish to receive fr	om the	interfaces						
Flow Configuration Table									
Q									
Device	Туре		IP Address	D	Tags	Traffic Statistics (FNF)		Voice/Video Performance (Medianet)	
B 🛞 DataCenter-WAN_EDGE	Standard	~	198.19.2.1	Cis	WAN, Ne	•	۵	۲	0
- S Ethernet0/0			198.19.2.1	Br	LAN			v	
Ethernet0/2	-		10.255.2.2	MPLS	1500, M	✓		✓	
BataCenter_Core	Standard	~	198.19.1.1	Cis	WAN, Lo	۲	۵	•	۵
- Ithernet0/0			198.19.1.1	Br	LAN			v	
- light Ethernet0/2			10.255.1.2	MPLS	1500, M	✓		v	
Remote_Site	Standard	~	198.18.129.25	Cis	WAN, Sa	۲	0	•	۵
- 🧐 Ethernet0/0			198.18.129.25		LAN			✓	
Ethernet0/1	-		10.255.0.2		1500, M	~		7	

Once the Performance Monitoring flow type is enabled, navigate to a device's real-time NetFlow view by clicking the "Flow" tab and then double-clicking on a device in the network map. Select the flow type drop down menu and select "Medianet."

QoS Flo	W Routing IP SL	A LAN						
Q Q 6	Enable Polling 🖙 F	Pause Display	Basic Flow	• 🖙 *	DefaultFilterGroup	👻 📑 Displa	y Filter Colors 👻	End Points: IP Address
Protocol	Src IP Addr	Src Port	All Flow Types	st Port	Application	In IF	Out IF	Src DSCP
TCP	2.2.2.2	23	Basic Flow	,233	skype	FastEthernet4	Vlan1	48 (CS6)
TCP	2.2.2.2	23	Medianet	,233	skype	FastEthernet4	Vlan1	48 (CS6)
UDP	123.123.123.2	161	Application (AVC)	,435	snmp	FastEthernet4	Vlan1	0 (BE)
UDP	123.123.123.2	161	10fb	,435	snmp	FastEthernet4	Vlan1	0 (BE)
UDP	123.123.123.2	62,624	1 Wireless	055	unclassified	FastEthernet4	Vlan1	0 (BE)
UDP	123.123.123.2	62,624	1 Uoknown	055	unclassified	FastEthernet4	Vlan1	0 (BE)
ICMP	123.123.123	-	152.100.0.2	2,816	icmp	FastEthernet4	Vlan1	48 (CS6)
ICMP	123.123.123	-	192.168.6.2	2,816	icmp	FastEthernet4	Vlan1	48 (CS6)
UDP	192.168.6.2	20,100	222.222.222.222	20,100	rtp	Vlan1	FastEthernet4	34 (AF41)
UDP	192.168.6.2	20,100	222.222.222.222	20,100	rtp	Vlan1	FastEthernet4	34 (AF41)
UDP	192.168.6.2	20,100	222.222.222.222	20,100	rtp	Vlan1	FastEthernet4	34 (AF41)
	197 168 6 2	20 100	<u>,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</u>	20 100	rtn	Vlan 1	FastEthernet4	34 (AE41)

The real-time Performance Monitoring flow records will now appear. Packet loss and jitter measurements will now be visible in the flow record. In the example below, two of the flows are being highlighted in pink due to an alarm being triggered by the cells in red. In this example, these flows Jitter Max measurements triggered an alarm. Network administrators are able to receive this performance alert via email or syslog message.

Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	DSCP and IP	RTP SSRC	Packet Loss Count	Packet Loss Percentage	Jitter Mean	Jitter Min	Jitter Max 1	-
192.168.6.2	20,000	222.222.222.222	20,000	ms-lync-media	46 (EP)	3219829004	0	0.00%	0.00 ms	0.00 ms	0.56 ms	
192.168.6.2	20,000	222.222.222.222	20,000	ms-lync-media	46 (EF)	3219829004	0	0.00%	0.00 ms	0.00 ms	0.56 ms	Ť.
192.168.6.2	20,000	222.222.222.222	20,000	ms-lync-media	46 (EF)	3219829004	0	0.00%	0.00 ms	0.00 ms	1.82 ms	1
192.168.6.2	20,000	222.222.222.222	20,000	ms-lync-media	46 (EF)	3219829004	0	0.00%	0.00 ms	0.00 ms	1.82 ms	2
192.168.6.2	20,100	222.222.222.222	20,100	rtp	34 (AF-41)	3176870698	0	0.00%	0.01 ms	0.00 ms	1.53 ms	1
192.168.6.2	20,100	222.222.222.222	20,100	rtp	34 (AF41)	3176870698	0	0.00%	0.01 ms	0.00 ms	1.53 ms	
192.168.6.2	20,100	222.222.222.222	20,100	rtp.	34 (AF41)	3176870698	0	0.00%	0.01 ms	0.00 ms	4.64 ms	2
192.168.6.2	20,100	222.222.222.222	20,100	rtp	34 (AF41)	3176870698	0	0.00%	0.01 ms	0.00 ms	4.63 ms	
192.168.6.2	20,000	222.222.222.222	20,000	ms-lync-media	46 (EF)	2254833084	0	0.00%	0.01 ms	0.00 ms	1.04 ms	
192.168.6.2	20,000	222.222.222.222	20,000	ms-lync-media	46 (EF)	2254833084	0	0.00%	0.02 ms	0.00 ms	1.06 ms	
192.168.6.2	20,000	222.222.222.222	20,000	ms-lync-media	0 (BE)	2254833084	N/A	N/A	N/A	N/A	N/A	
197 168 6 7	20.000	777 777 777 777 III	20.000	me-luni-marka	0 (RF)	2254833084	N/A	N/A	N/A	N/4	N/A	5



APPENDIX C: SKYPE QOS AUDIO CONFIGURATION USING NBAR2 DEFINITIONS

LiveNX and NBAR2 makes protecting Skype traffic extremely easy. Earlier in this guide, methods were described on how to recognize and mark ingress traffic using ACL's to identify ports used for Skype audio or video. This required changes to the Microsoft servers and clients. With NBAR2 protocol pack 12 (or higher) that is no longer necessary. NBAR2 applications can be applied directly to QoS polices using the LiveNX QoS Management GUI.

Begin by creating an ingress to QoS Policy to Classify Skype Audio as DSCP 46. To do this, open the LiveNX Manage QoS Settings window.

Device: Branch1-LA.dcloud.cisco.com)	
QoS	· ·	Enable QoS Polling
Flow	· · -	Manage QoS Settings
Routing	•	Revert QoS Configuration
IP SLA	•	Manage NBAR
LAN		Apply Policy to Interfaces
Edit Device Settings		Remove Policy from Interfaces
Add or Remove Interfaces		Copy Policy to Devices
Refresh Device		Reports
Remove Device		
Zoom to Device		
Device Tools	•	_
Statistics	•	
View	•	-
Group Management	•	





Create a new QoS Policy by selecting "Add Policy" and give the policy a name.

cies	Mapped Classes	
LIVEACTION-POLICY-UNIFIED	Class Name Classify Marking Queueing Policing Shaping Comp	ression WRED DBL Unknow
	Mapped C Add Policy X Drop a Classify Policy name: SET_DSCP on WRED DD	BL Unsupported
	Match or OK Cancel	Reference Class is defined by the criteria show at left. Match-any: packet must meet at least one of the criteria to be a member of the class.
	Frite	Match-all: packet must mee all criteria to be a member of the class.

After creating the new policy, right click on the new policy and select "Add Class to Policy."

A Manage QoS Settings - SC-4331-V	VAN (10.10.20.1)								×
ତି 🗐 🗿 🗿 🖓 🗞									
Policies Classes Interfaces									
Policies	Mapped Classes								
LIVEACTION-POLICY-UNIFIED	Class Name Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
clas Copy Policy									
Add Class to Poli	<mark>cy </mark>								
Apply Policy to Ir	nterface								
🗧 Remove Policy fr	om Interface								
	Classify Marking Que	eueing Polic	ing Shapin	g Compre	ession WR	RED DBL Unst	upported		
			Ed	ł		Cite cri me cri the M all the	ass is defi teria shov atch-any: teria to be e class. atch-all: p criteria to e class.	ned by vat left packet one of a mem acket n be a m	the must the ber of nust meet ember of
Help				Save to	Device	Preview C	u	c	ancel

Give the new class a name.

-	
 Use existing class: 	LIVEACTION-CLASS-AVC ~
Create new class:	Skype-Audio
Note: This option w	ill create an empty class. You will

Next, select "Edit" to add Skype audio to the class.

A Manag	ge QoS Settings - R	emote_Sit	te.dcloud.	cisco.cor	n (198.1	8.129.25)			×
ට් 🗐 🗿 🖏 🖏 🚳 🍕									
Policies Classes Interfaces									
Policies	Mapped Classes								
🛃 🐂 📚 🔝 🐜 🐃 👒 🗠	98 🗈 🖪 🖮								
LIVEACTION-POLICY-MEDIANET	Class Name Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
SET_DSCP	Skype-Audio 🧅								
Skype-Audio	Cass-default								
Cass-default									
	Mapped Class Detail								
	Drop all traffic for d	ass							
	Classify Marking Qu	eueing Pol	icing Shapin	og Compre	ession WR	ED DBL Unsu	upported		
	Match on: Any					Ref	erence		
						Cla	iss is defi	ined by	the
						cri	teria snov	vatien	
						Ma	atch-any:	packet	must
						cri	teria to be	a mem	ber of
						the	class.		
						Ma	atch-all: p	acket n	nust meet
						all	criteria to class.	be a m	ember of
			Ed	it					
< >									
Help				Save to	Device	Preview C	u	C	ancel

LiveAction

On the Class Tab, select "Protocol–using NBAR" as the match type. Then select "ms-lync-audio" as the NBAR application, and then select "Add Match Statement."



Now, go back to the Policies tab, and then select the Marking tab. On the Marking tab check the box for DSCP and select "46 (EF)."





Now add another "class" to the SET_DSCP policy to mark our Skype video traffic as DSCP 34.

	Add	Class to Policy	×							
Select one	of the followi	ing options:								
O Use ex	isting class:	LIVEACTION-CLASS	-AVC 🗸							
Create	Create new class: Skype-Video									
Note: 1 need t parame	This option wi o select the " eters.	ill create an empty cla Class tab [®] to add clas	ss. You will sification							
		OK	Cancel							

After creating the new class please select "Edit."

A Manag	ge QoS Settings - F	lemote_Site	.dcloud.o	cisco.cor	n (198.1	8.129.25)			×
2 1 2 2 2 2 4 5									
Policies Classes Interfaces									
Policies	Mapped Classes								
🛃 🖷 🏽 👪 🌆 🖷 📬 🎼	PB 💁 📗 🖮								
LIVEACTION-POLICY-MEDIANET	Class Name Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
SET DSCP	Skype-Audio 🛛 👳	DSCP: EF							
Skype-Audio	Skype-Video 🔶								
Skype-Video	class-default 👳								
dass-default									
	Mapped Class Detail								
	Drop all traffic for o	lass							
	Classify Marking Q	ueueing Polici	ing Shapin	g Compre	ession WR	ED DBL Unsu	pported		
	Match and Ann	-				0.6			
	Match on: Any			_		Ker Cla	erence	ined by	the
						cri	teria shov	v at left	
						Ma	et at least	packet	the
						cri	teria to be	a mem	ber of
						the	class.		
						Ma	atch-all: c	acket r	nust meet
						all	criteria to	be a m	ember of
			Edi	the state		the	class.		
				~]					
< >									
Help				Save to	Device	Preview C	u	c	ancel

Once on the class tab please select the match type to be "Protocol–using NBAR" and then select "ms-lync-video" and lastly "Add Match Statement."

A	Manage	QoS Settings - Remote_Site.dcloud.cisco.co	m (198.1	8.129.25)		
44223	🗞 🖏					
Policies Classes Int	terfaces					
Classes	Create and Edit Ma	tch Statements				
📴 🗓 😹	Match type:	Protocol - using NBAR	Ma	tch any 🗸	*	
LIVEACTION-CLAS	rider cyper					
LIVEACTION-CLAS	Value:	msg-auth	^ M	Match T	Value	
Skype-Audio		msg-icp medic	Ma	. Protocol	ms-lync-video	
Skype-video		ms-live-accounts	_			
		ms-lync				
		ms-lync-audio				
		ms-lvnc-media	a.			
		ms-lync-video	~			
	Match/match not:	Match	~			
	L	Add Match Statement	t			
Help		Save to	Device	Preview	CLI C	ancel

Go back to the "Policies Tab" and select the "Marking Tab" to properly mark Skype video as DSCP 34.

Mana	ge QoS Settings - R	emote_Site.do	loud.cisco	.com (198.1	8.129.25)			
 2 ● ● ● ● ● Policies Classes Interfaces 								
Policies	Mapped Classes							
등 제 🖹 🍰 🏭 제 🖏 🕫	🕒 😭 🐘 📄							
EIVEACTION-POLICY-MEDIANET	Class Name Classify	Marking Que	ueing Polici	ing Shaping	Compression	WRED	DBL I	Unknown
LIVEACTION-POLICY-UNIFIED	Skype-Audio 🔹	DSCP: EF						
Skype-Audio	Skype-Video 🛛 👳	DSCP:						
	dass-default 👳							
dass-default								
	Mapped Class Detail							
	Drop all traffic for di	ass						
	Classify Marking Qu	eueing Policing	Shaping Co	ompression WR	ED DBL Uns	upported		
	Mark with:				Re	ference		
		26 (4521)			D	fferentiate	packets	^
	USCP	V 20 (AF31)	v .		bi	ased on ma	rking.	5
	IPv4 Onl	у				anti On		
	ATM Cell Loss	Priority			-	ark On		_
	Frame Relay	Discard Eligible			D	SCP: marks etting the di	s a packe ifferential	t by ted
					s	ervices cod	de point	
					(0	SCP) value service (T	e in the ty OS) byte	pe
					P	ecedence	e: sets th value in t	he V
< >					<			>
Help			Sav	ve to Device	Preview	u	Car	ncel

LiveAction

Now with a policy to identify and mark the Skype audio and video, apply the new policy to an interface by right-clicking on the policy and selecting "Apply Policy to Interface."

Mar	age QoS Setting	s - HQ-SJ.	dcloud.cis	co.com	(198.18.	129.25)			
2 2 2 2 2 2 2									
Policies Classes Interfaces									
Policies	Mapped Classes								
📑 🗓 😹 🔝 🔚 🗳 👒									
LIVEACTION-POLICY-UNIFIED	Class Name Classi	y Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
V Copy Policy		DSCP: EF							
Delete Policy		0307							
Add Class to Policy	6								
Apply Policy to Interpolicy 10 Interpolicy	aface								
Remove Policy from	n Interface								
	Drop all traffic for Classify Marking C Mark with: DSCP DPv4 C ATM Cell Lo Frame Relat	dass (ueueing Po y 34 http: ss Priority y Discard Eligit	icing Shapir (AF41)	ng Compr	ession (Wi	ED DBL Uns Ref Db bb bb bb bb bb bb bb bb bb bb bb bb	apported ference fferentiate longing to sed on m ark On CP: mark tting the c rvices co SCP) valu service (eccedence	e packets this class arking. S a pack differenti de point re in the TOS) by ce: sets	s ^ SS ket by iated type te. the the the s
Help				Save to	Device	Preview C	u [c	ancel

Select the interface to apply the policy to and select "OK."

Apply Policy to Interfaces	×
Select a policy: <u> EET_DSCP</u>	~
Select the interfaces to which you want to apply this policy: GigabitEthernet0 GigabitEthernet0/0/0 GigabitEthernet0/0/0 GigabitEthernet0/0/1 GigabitEthernet0/0/1 Output Output	
OK Canc	el



Lastly, select "Save to Device" to apply the policy to the device itself.

A Mana	ge QoS Settin	ngs - Re	mote_Sit	e.dcloud.	cisco.co	m (198.1	8.129.25)			×
ତ୍ରି 🗐 🗿 🖏 🖏 🗞 🦠										
Policies Classes Interfaces										
Policies	Mapped Classes	s								
🛃 🕷 😹 🐜 📲 🛝 🔫	P3 🖿 🚯 🛛	<u> </u>								
LIVEACTION-POLICY-MEDIANET	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
SET_DSCP	Skype-Audio	۲	DSCP: EF							
Skype-Audio	Skype-Video dass-default		DSCP:							
Skype-Video										
	Mapped Class D	Detail								
	Drop all traf	ffic for cla	ss							
	Classify Mark	king Oue	ueing Pol	cing Shapir		ession WF	ED DBL Uns	upported		
	Match on: An						Pe	ference		
	Match / Droto	y col - ucior		Junc-audio	_		C	ass is def	ined by	the
	Matur: Proto	coi - using	NDAR . III	-Tyric-doulo			cr	iteria show	w at left	t.
							M	atch-any:	: packet	must
							m	eet at leas	t one o	fthe
							cr th	e class.	e a merr	ber of
							M	atch-all: p criteria to	be a m	must meet ember of
				Ed	it		th	e class.		
< >>	L									
Help					Save to	Device	Preview	CLI	C	ancel
						<u></u>				

APPENDIX D: SKYPE QOS QUEUING WITH LIVENX AND NBAR2

Now that Skype audio and video were easily identified and marked in the SET_DSCP Policy, create a queuing policy to protect the traffic.

From the "Manage QoS Settings" on the device that would need a queuing policy applied to, start by creating a new policy.

Manag	ge QoS Settings - Remote_Site.dcloud.cisco.com (198.18.129.25)
진 휜 බ බ බ 이 영 특	
Policies	Mapped Classes
Add Policy N-POLICY-MEDIANET	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unknown
SET_DSCP Skype-Audio Skype-Video dass-default	Skype-Video © DSCP: dass-default ©
	Mapped Class Detail Drop all traffic for class Classify Marina Queueing Policing Shaping Compression WRED DBL Unsupported
	Match on: Any Reference
	Match : Protocol - using NBAR : ms-lync-audio Class is defined by the criteria show at left. Match-any: packet must meet at least one of the criteria to be a member of the class. Match-all: packet must meet all criteria to be a member of the class. Edit Edit Match-all: packet must meet all class one of the class.
< >	
Help	Save to Device Preview CLI Close

Call the new policy "queuing."



Live Action **



Right click on the new "queuing" policy and select "Add Class to Policy."

Ma 1 4 5 5 5 6 5	nage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)	
blicies Classes Interfaces		
olicies	Mapped Classes	WRED DBL Unknow
Apply Policy <u>Add Cla</u> Remove Policy from	Interface Mapped Class Detail Drop all traffic for class Classify Maring Queueing Policing Shaping Compression WRED DBL Un	supported
	Mark with:	eference Differentiate packets ^ lelonging to this class lased on marking. Mark On
	Frame Relay Discard Eligible	OSCP: marks a packet by tetting the differentiated tervices code point DSCP) value in the type of service (TOS) byte.
	3	Precedence: sets the recedence value in the C >

Give the new class a name.

🛕 Add Class to Polic	y X
Select one of the followi	ng options:
O Use existing class:	LIVEACTION-CLASS-AVC 🗸 🗸
Create new class:	VOIP
Note: This option wi need to select the " parameters.	ll create an empty class. You will Class tab" to add classification
	OK Cancel



After the new policy is created select "Edit" to match on the DSCP 46 markings.

Manag	ge QoS Sett	ings - Re	emote_Si	te.dcloud.	cisco.co	m (198.1	8.129.25)			×
ତ୍ରି କି କି କି କି 🖗 🔍										
Policies Classes Interfaces										
Policies	Mapped Class	es								
		•								
UVEACTION-POLICY-MEDIANET	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
QUEUEING	VOIP	•								
	Cass-Gerauit									
E SET_DSCP										
Skype-Audio										
dass-default										
	Mapped Class	Detail								
	Drop all tr	affic for cla	ISS							
	Classify Ma	arking Qu	eueing Pol	icing Shapir	ng Compr	ession WF	RED DBL Unsi	upported		
	Match on: A	ny					Ref	erence		
							Cla	ass is defi	ined by v at left	the
								teria arren	at lon	
							Ma	et at leas	packet tone of	must the
							cri	teria to be	a mem	ber of
							the	e class.		
							Ma	atch-all: p	be a m	nust meet
				E	64. T		the	class.	be a m	ember of
					<u>الم</u>					
x										
Help					Save to	Device	Preview C	u	(ancel

On the "Classes Tab" select "DSCP" as the "Match Type." Select "46 (EF)" as the value, and then "Add Match Statement" to those markings.

A Mana	ge QoS Settings - Remote_Site.dcloud.cisc	p.com (198.18.129.25)
44444		
Policies Classes Interfaces		
Classes Create and Edit !	latch Statements	
🕒 🛈 🕱 🛛 Match typ	e: DSCP	V Match any V
LIVEACTION-CLAS	e: 39	A M Math T Value
Skype-Audio	40 (CS5)	Ma DSCP 46 (EE)
Skype-Video	41	
VOIP	42	
	43	
	45	
	46 (EF)	✓
	(Select up to 8 values)	
Match/match no	t: Match	~
	IPv4 Only	
	Add Match Statement C	ement
Help	Sa	ave to Device Preview CLI Cancel



After selecting the correct match type, please go back to the "Policies Tab" and then select the "Queuing Tab" for the VOIP Class. Set the priority bandwidth percentage to 33%. This is a safe starting number for this queue, and can be adjusted by monitoring the queue performance over time.

Policies Classes Interfaces									
Policies	Mapped Classes								
🛃 🖄 📸 🛼 🐘 🖄 🛸 🖷	Pe 🖹 📑 🖷								
	Class Name Cla	assify Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unkno
LIVEACTION-POLICY-UNIFIED	VOIP	•	Priority: 3						
	class-default	•							
dass-default									
E SET_DSCP									
Skype-Video									
dass-default									
	Mapped Class Det	ail I							
	Drop all traffic	for class							
	Classify Marking	Queueing Po	olicing Shapin	ng Compr	ession WF	RED DBL Uns	upported		
		Priority v				Re	ference		
	Quedenig type:	(indite)				Di	stribute th	e availal	ble
	Rate: 33	Percer	nt 🗸			ba	indwidth t	etween	
	Burst siz	e: 32	bytes			Ci m	nimum bar	ndwidth	nga
	Unknown ele	ments:				gu	arantee to	each c	lass.
						0	ueueina	Type	
						-	ace has	ad: utiliz	40
						C	ass-based	d weight	ted fair
						qu	eueing (C	BWFQ)	using
						de fr	mixed wei	ght for p ndwidth	ackets
						al	ncated to	the clas	•

Create a second video class to the policy to protect Skype video.

🛕 Add Class to Polic	y	×
Select one of the followi	ng options:	
O Use existing class:	LIVEACTION-CLASS-AV	c ~
Oreate new class:	VIDEO	
Note: This option wi need to select the " parameters.	ll create an empty class. Class tab" to add classific	You will ation
	OK	Cancel



Select "Edit" for to correctly classify video traffic DSCP 34.

A Mana	ge QoS Set	tings - Re	emote_Si	ite.dcloud.	cisco.co	m (198.1	8.129.25)			×
🗐 🗐 🖣 🖏 🖏 🍪 🎭										
Polices Polices CUERACTION-POLICY-ADIANET QUEUEING VOIP VOIP VOIP VOIP VOIP VOIP VOIP VOIP VOIP Skype-Audo Skype-Audo Skype-Audo Skype-Audo	Mapped Classes									
	Class Name VOIP	Classify	Marking	Queueing Priority: 3	Policing	Shaping	Compression	WRED	DBL	Unknown
	class-default	•								
	Mapped Class Detail Drop all traffic for class									
	Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported Match on: Any Reference									
	Class is criteria						ass is def iteria shov	s defined by the show at left.		
	Match-any; pa met at least or criteria to be a the class.							t one of a mem	must the ber of	
				Ed	i v C		M all the	atch-all: ; criteria to e class.	packet r be a m	nust meet ember of
< >					Save tr	Device	Preview (11		ancel
nep					Save u	Device	Freview C			dillei

On the classes tab please select "DSCP" as the match type, "34 (AF41)" as the value, then select "Add Match Statement."

A	Manage	QoS Settings - Remote_Site	dcloud.cisco.com (1	98.18.129.25)	
44999	8				
Policies Classes In	terfaces				
Classes	Create and Edit Ma	tch Statements			
🔁 🗓 😹	Match type:	DSCP	~	Match any 🗸 🗱	
LIVEACTION-CLAS	Value:	27	0	M Match T Value	
Skype-Audio		28 (AF32)		Ma DSCP 34 (AE41)	
Skype-Video		29			
VIDEO		30 (AF33)			
VOIP		32 (CS4)			
		33			
		34 (AF41)	×		
		(Select up to 8 values)			
	Match/match not:	Match	~		
		IPv4 Only			
		Add Match Statement	lace Match Statement		
< >					
Help			Save to Devic	ce Preview CLI Cancel	

After selecting the correct match type, select the "Policies Tab" and then select the "Queuing Tab" for the video class. Set the bandwidth percentage to 20%. This is a safe starting number for this queue, and can be adjusted by monitoring the queue performance over time.



The queuing policy can now be applied to an interface.

Manag	ige QoS Settings - Remote_Site.dcloud.cisco.com (198.18.129.25)					
ତ୍ର କା କା କା କା 🐁 🦠						
Policies Classes Interfaces						
Policies	Mapped Classes					
🔄 🗓 😹 🏡 🐜 🗳 👒						
LIVEACTION-POLICY-MEDIANET	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unknown					
	VOIP Priority: 3					
Copy Policy	Class-bas					
Delete Policy						
Add Class to Policy						
Apply Policy to Inter	iface					
Remove Policy from	n Interface Apply Policy to Interface					
	Drop all traffic for class					
	Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported					
	Outputing types [Class based up					
	Distribute the available					
	Rate: 20 Percent V bandwidth between					
	Queue depth: 1 Bytes V Classes by specifying a minimum bandwidth					
	Enable Fair Queueing guarantee to each class.					
	Unknown elements: Queueing Type					
	Class-based: utilizes Class-based weighted fair queueing (CBWFQ) using derived weight for packets from the bandwidth all-rated to the class <					
Help	Save to Device Preview CLI Cancel					





Add the policy to the correct interface.



"Save the policy" when completed.

A Manag	ge QoS Settings - Remot	e_Site.dcloud.	cisco.co	m (198.1	8.129.25)			×
E a a a a a a a a								
Policies	Mapped Classes							
C LIVEACTION POLICY MEDIANET UNEACTION POLICY MEDIANET VOID VOID VOID VOID Skype-Mideo dass-default Skype-Video dass-default	Class Name Classify Mar VOIP VIDEO class-default	ring Queueing Priority: 3 Class-bas	Policing	Shaping	Compression	WRED	DBL	Unknown
	Mapped Class Detail Drop all traffic for class Classify Marking Queueing Queueing type: Class-basec Rate: 20 P Queue depth: 1 Enable Fair Queuein Unknown elements:	Policing Shapin	ig Compr	ession WF	RED DBL Unst Ref Dia cla mi gu QU CL	ipported erence stribute the ndwidth b isses by s nimum ban arantee to jeueing 1 ass-base	e availabi etween pecifyin dwidth each cla Fype d: utilize	le ^ g a ass.
	Class-based weighted fair queueing (CBWFO) using derived weight for packet from the bandwidth allingtated in the class c						ed fair using ackets	
Help			Save to	Device	Preview C	u	Ca	incel

MORE INFORMATION

<u>QoS</u>

Find out more about QoS including best practices and the latest tools for monitoring and creating new policies.

Upcoming Webinars

Check out our updated webinar schedule—gain insights from our special presenters about topics like QoS, Hybrid WAN Management, Capacity Planning and more.

Additional Resources

Case studies, white papers, eBooks and more are available for your learning on the LiveAction resources page.

LiveNX and LiveUX Downloads

Free downloads of <u>LiveNX</u> and <u>LiveUX</u> are available now. Visit our webpage to discover more details and benefits of LiveNX and LiveUX.

ABOUT LIVEACTION

LiveAction provides comprehensive and robust solutions for Network Performance Management. Key capabilities include Cisco Intelligent WAN visualization and service assurance, best-practice QoS policy management, and application-aware network performance management. LiveAction software's rich GUI and visualization provide IT teams with a deep understanding of the network while simplifying and accelerating management and troubleshooting tasks.

©2016 LiveAction, Inc. All rights reserved. LiveAction, the LiveAction logo and LiveNX Software are trademarks of LiveAction. Other company and product names are the trademarks of their respective companies.

LiveAction, Inc. · 3500 West Bayshore Road · Palo Alto, CA 94303 · USA · +1 (888) 881-1116